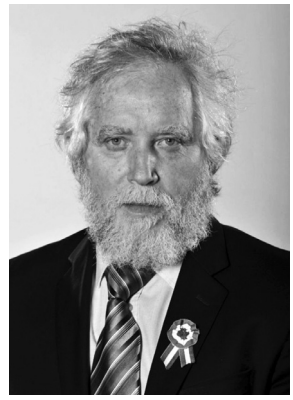
Endre Szemerédi – Abelov laureat za 2012. godinu

Darko Veljan[1]

Uvod



Na svečanoj dodjeli Abelove nagrade 22. svibnja 2012. godine u Oslu, norveški ju je kralj Harald za 2012. godinu dodijelio mađarsko-američkom matematičaru Endre Szemerédiju, članu Instituta za matematiku "Alfred Rényi" iz Budimpešte i profesora odsjeka za računarstvo, odnosno izvorno na Department of Computer Science, Rutgers University, New Jersey, SAD.

Endre Szemerédi je Abelovu nagradu dobio za svoje temeljne i trajne doprinose u diskretnoj matematici i teorijskom računarstvu, kao i za zasluge zbog velikog značaja koji su njegovi radovi ostavili u aditivnoj teoriji brojeva i teoriji ergodičnosti. (O Abelovoj nagradi vidi članak D. Veljan, John Milnor – dobitnik Abelove nagrade za 2011. godinu, MFL 62, br. 3 (2011./ 12.), 172–176, i literaturu u tom članku).

Diskretna matematika, kombinatorika i teorija grafova

Pokušajmo prvo ukratko opisati glavno područje djelovanja prof. Szemerédija.

Diskretna matematika kao jedna od temeljnih grana matematike prvenstveno proučava diskretne strukture.

Za razliku od neprekidnih struktura (npr., realnih i kompleksnih brojeva **R** i **C** i matematičke analize na njima, te geometrije i topologije), diskretne strukture su skupovi

[1] Redoviti profesor u mirovini na Matematičkom odsjeku Prirodoslovno-matematičkog fakulteta u Zagrebu; e-pošta: darko.veljan@gmail.com

na kojima razlikujemo svaku točku od njenih susjeda (a razlikujemo i same susjede). Primjerice, susjedne točke od nule u skupu $\mathbf{Z}$ cijelih brojeva su -1 i $+1$. Stoga skup $\mathbf{Z}$ (zajedno s pripadnim aksiomima) čini jednu diskretnu strukturu. Slično je i skup $Z \times Z$ – rešetka parova cijelih brojeva (x, y) – također diskretna struktura (kao i svaki njezin podskup), jer oko svake točke (x, y) imamo četiri susjeda. Dakako, svaki je konačan skup također diskretan. U stvari, oko svake točke diskretnog skupa u nekom prostoru, postoji okolina u kojoj nema drugih točaka tog skupa.

U čitavom korpusu diskretne matematike posebno je važan dio koji se zove kombinatorika. Tipična (srednjoškolska) pitanja u kombinatorici su pitanja prebrojavanja. Evo par primjera. Na koliko se načina elementi konačnog skupa $[n] = \{1, 2, \ldots, n\}$ mogu poredati u niz? (Odg. $n! = 1 \cdot 2 \cdot \ldots \cdot n$.) Ili, koliko ima k-članih podskupova u n-članom skupu $[n]$? (Odg. $\binom{n}{k} = n!/k!(n-k)!$.) Koliko ima funkcija, a koliko injekcija, i koliko surjekcija iz jednog u drugi konačni skup? (Odg. funkcija $[k] \to [n]$ ima n^k, od toga injekcija ima $n(n-1)\ldots(n-k+1)$, a surjekcija $[n] \to [k]$ ima $k!S(n,k)$.) Na koliko se načina skup $[n]$ može rastaviti u k blokova (nepraznih disjunktnih podskupova)? (Odg. $S(n,k)$ – Stirlingov broj druge vrste.)

U kombinatorici i uopće u diskretnoj matematici, jedna od uvijek vrućih tema su rekurzije. Primjerice, poznata Pascalova formula $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$ je rekurzija iz koje možemo postupno izračunavati binomne koeficijente počevši od početnih vrijednosti $\binom{0}{0} = \binom{1}{0} = \binom{1}{1} = 1$ i $\binom{n}{k} = 0$ za $k > n$. Slično, za Stirlingove brojeve druge vrste vrijedi rekurzija $S(n+1,k) = kS(n,k) + S(n,k-1)$, uz početne uvjete $S(0,0) = 1$, $S(n,0) = S(0,n) = 0$, za $n > 0$.

Drugo važno područje diskretne matematike je teorija grafova. Graf je naprosto neki (konačan) skup točaka – vrhova i nekoliko njihovih spojnica – bridova. Dva vrha spojena bridom zovu se susjedni. Stupanj vrha je broj njegovih susjeda. Na primjer, graf prijateljstava među 30 ljudi (recimo, učenika nekog razreda) sastoji se od 30 vrhova, a bridom su spojene dvije točke koje predstavljaju parove prijatelja. Kocku možemo shvatiti kao graf s 8 vrhova (svaki stupnja 3) i 12 bridova (a kocku dimenzije n kao graf s 2^n vrhova i $n \cdot 2^{n-1}$ bridova, svaki vrh je stupnja n). U potpunom grafu od n vrhova, svaka su dva vrha spojena bridom. To je kao n-terokut sa svim dijagonalama.

Grafovima se mogu modelirati i simulirati mnoge prirodne i druge aktivnosti i situacije, pa se tako teorija grafova kao čista teorijsko-matematička disciplina primjenjuje ne samo u matematici (recimo u teoriji kodiranja), te u računarstvu i informatici, nego i inžženjerstvu, ekonomiji, medicini, prirodnim znanostima (fizika, kemija, biologija,..) pa i u društvenim znanostima i lingvistici i drugdje. (Zadatak za čitatelje. Pomoću grafova dokažite tzv. lemu o rukovanju: na svakom "tulumu" broj ljudi koji su se rukovali s neparnim brojem drugih je paran broj. Uputa. Promotrite zbroj stupnjeva svih vrhova grafa rukovanja.)

Evo i jedne konkretne primjene grafova u računarstvu, a odnosi se na paralelno računanje. Podsjetimo se prvo (ili podučimo one koji ne znaju) da se Fibonaccijevi brojevi definiraju rekurzijom $F(n+1) = F(n) + F(n-1)$, uz početne uvjete $F(0) = 0$ i $F(1) = 1$. Tako je npr. $F(6) = 8$, $F(7) = 13$, a $F(8) = 21$. Fibonaccijeva kocka je graf koji ima Fibonaccijev broj vrhova i temeljna je tvorevina za topologiju mreže po kojoj se odvijaju paralelna računanja.

Postoje naizgled i vrlo jednostavni problemi koje ni masovno paralelno računanje ne može razriješiti. Tipičan je takav problem trgovačkog putnika (PTP). Trgovački putnik

treba obići n gradova, svaki samo jednom i vratiti se natrag na početak. Poznate su mu sve razdaljine među gradovima, a on želi pronaći najkaraći put. Ni danas se ne zna dobar algoritam za PTP, tj. takav algoritam za kojeg postoji polinom u n i razdaljinama kojima se izražava broj učinjenih osnovnih operacija prilikom rada algoritma na nekom zadatku. Za $n = 1000$ gradova, s izravnom – "naivnom" metodom nalaženja najkraćeg puta uspoređivanjem duljina svih putova trebali bi milijuni godina rada svih današnjih računala umreženih paralelno. Stoga je potraga za algoritmom koji radi u "realnom vremenu" od presudne važnosti, a ne samo "zaigranost" matematičara.

PTP je duboko vezan za najvažnija pitanja (teorijskog) računarstva, posebno s najpoznatijim otvorenim pitanjem: "Je li $P = NP$"? Grubo rečeno, problem se može izreći ovako. Da li svaki problem čije rješenje možemo brzo kompjutorski provjeriti, možemo tada brzo kompjutorski i riješiti? PTP zapravo pita postoji li polinomski algoritam za nalaženje najkraćeg (najlakšeg) Hamiltonovog ciklusa u potpunom težinskom grafu.

Prava je šteta da se danas u srednjoškolskoj nastavi više gotovo ništa ne uči o kombinatorici i uopće o diskretnoj matematici kako smo je ukratko pokušali opisati. No, to je već neka druga tema. (Zainteresirani čitatelji osim na internetu, mogu na hrvatskome jeziku pogledati udžbenik D. Veljan, Matematika za 4. razred gimnazije, Školska knjiga, Zagreb, 2000, ili sveučilišni udžbenik D. Veljan, Kombinatorna i diskretna matematika, Algoritam, Zagreb, 2001.)

Szemerédijev teorem o aritmetičkim nizovima

Vratimo se laueratu-profesoru E. Szemerédiju. Predavanje koje je održao prilikom dodjele Abelove nagrade imalo je naslov: "In every chaos there is an order", ili u slobodnom prijevodu: u svakom neredu ima reda. Najveći dio predavanja posvetio je svojem teoremu o aritmetičkim nizovima iz 1975. Teorem kaže da svaki podskup prirodnih brojeva s pozitivnom gornjom gustoćom ima po volji dugačak aritmetički niz. Sjetimo se, aritmetički niz brojeva je niz kojemu je razlika susjednih članova stalna (konstantna). Aritmetički niz duljine k izgleda ovako: a, $a+d$, $a+2d$, $a+3d$,..., $a+(k-1)d$. Spomenimo za one koje to zanima da je gornja gustoća podskupa S prirodnih brojeva definirana kao $\lim \sup(\#(S \cap [n])/n)$, kada n teži u beskonačnost $(n \to \infty)$; simbol # čitaj: broj elemenata.

A što znači da skup S sadrži po volji dugačak aritmetički niz? To znači da kakav god prirodni broj uzeli, recimo 1234, onda skup S sadrži aritmetički niz duljine barem 1234.

Szemerédijev se teorem o aritmetičkim nizovima može izreći i ovako. Za svaki broj g ("gustoća"), $0 < g < 1$, i svaki prirodni broj k, postoji broj $N(g,k)$, tako da za svako $N > N(g,k)$, svaki podskup iz $\{1,2,\ldots,n\}$ od gn elemenata ima aritmetički niz duljine k.

U dokazu teorema, kao ključni korak prvo je dokazao tvrdnju poznatu kao Szemerédijeva lema o regularnosti. Ta je lema imala vrlo velik značaj u kombinatorici, teoriji grafova, aditivnoj teoriji brojeva, informatici i teorijskom računarstvu, diskretnoj geometriji, teoriji vjerojatnosti, teoriji ergodičnosti i drugdje.

Spomenimo ovdje i sljedeći nedavno dokazani teorem (B. Green i T. Tao, 2009): Niz prostih brojeva 2, 3, 5, 7, 11, 13, 17, 19, 23, 29,... sadrži aritmetički niz bilo koje duljine, pa stoga i po volji dugačak.

Osim teorema o aritmetičkim nizovima, Szemerédi je dokazao i druge važne rezultate. Poznat je tako Szemerédi-Trotterov teorem iz diskretne geometrije o najvećem mogućem broju incidencija od n točaka i m pravaca (tj. broj parova točka – pravac tako da je točka na pravcu) i iznosi otprilike $(mn)^{\frac{2}{3}}$. Poznat je također i Erdös-Szemerédijev teorem i drugi.

Isto je tako poznat i sljedeći teorem o presječnom broju grafa. Ako u ravnini bilo kako nacrtamo (jednostavni) graf koji ima n vrhova i m bridova, $m > 4n$, onda je najveći broj presjecišta bridova (osim vrhova grafa) najviše jednak $m^{\frac{3}{64}}n^2$.

Ustvari, iz ovog teorema o presjecištima lagano slijedi gornji teorem o incidencijama.

Osim navedenih, Szemerédi je imao i drugih rezultata i zasigurno će mnogi od njih ući u trajnu baštinu povijesti znanosti.

Kratka biografija

Endre Szemerédi je rođen 1940. u Budimpešti. Već je u gimnaziji pokazao izrazite matematičke sposobnosti. Diplomirao je matematiku na Eötvös Loránd Sveučilištu u Budimpešti, a doktorirao na MGU (Državno Sveučilište) u Moskvi u Rusiji. Voditelj doktorata bio mu je čuveni matematičar Israel M. Gel'fand (1913.–2009.). Od 1974. gotovo stalno živi i radi u SAD-u, a od 1986. profesor je na spomenutom Rutgersu.

Član je Mađarske akademije znanosti od 1987., te Nacionalne akademije znanosti SAD-a od 2010. Stalni je član čuvenog Institute for Advanced Study (Zavod za napredna istraživanja) u Princetonu, NJ. Objavio je oko 200 znanstvenih radova. I prije Abelove, za svoje je znanstvene doprinose dobio više nagrada. Primjerice, Grünwaldovu 1967., Rényijevu 1973., Steelovu nagradu 2008. i druge. Szemerédi je imao 11 doktorskih studenata. Oženjen je i otac petoro djece.

Kažimo da je zapravo njegov pravi učitelj bio poznati matematičar Paul Erdös (1913.–1996.). Szemerédi je riješio jedan od težih Erdösevih problema i tako "zaradio" 1000\$. U stvari, Szemerédijev teorem o aritmetičkim nizovima je bila Erdös-Turánova slutnja iz 1936. godine. (O životopisnom i legendarnom Erdösu vidi članke D. Veljan, Paul Erdös, Matka 24 (1998), 186–191 i V. Devidé, P. Erdös – "šašavi" genijalac, Matka 32 (2000), 92–96.)

Ključne znanstvene ideje

Osnovne znanstvene zamisli Szemerédijeve "matematičke filozofije" možemo grubo izreći ovako. U svakom (gotovo) kaotičnom, nepravilnom, iregularnom skupu S, uvijek postoji neki potpuno pravilan, regularan kutak A, i koji je pritom dovoljno velik. Skup S u nekom smislu mora biti gust, tj. mora zadirati u gotovo svaki djelić cjeline (diskretne strukture) u kojoj sve to promatramo, recimo u skupu N prirodnih brojeva.

Tako, primjerice, možemo zamisliti da je učinjena neka vrsta matematičke dezinfekcije kojom je uklonjeno 99.999% slučajno odabranih prirodnih brojeva. Tada će preostalih 0.001% preživjelih brojeva sadržavati po volji dugačak aritmetički niz.

Dakle, iako se S može učiniti naizgled kaotičnim, gotovo pa slučajnim, ipak u njemu postoji pravilni dio.

Glavna ideja dokaza (među ostalima i Szemerédijeve leme o regularnosti) je u grubim crtama sljedeća. Svaki veliki sustav rastavimo na mnogo malih komadića približno iste veličine koji su naizgled slučajno odabrani. To onda omogućava proučavanje globalnog složenog sustava bez zadiranja u sve pojedinosti malih komadića. Kao primjer, možemo zamišljati hiperlinkove kao male komadiće u globalnoj mreži `world wide web-www`; tako ipak znamo globalnu strukturu mreže, a da pritom ne moramo znati svaki detalj svakog linka.

A na kraju se tu puno zaključaka svodi na jednostavno Dirichletovo načelo (princip), koji u svojoj najjednostavnijoj izreci kaže da je uvijek među troje ljudi, bar dvoje njih istog spola. Ili, ako je u 4 golubinjaka ukupno 5 golubova, onda je u bar jednome golubinjaku bar dvoje golubova. Ili, u stilu poznate šale, ako iz vlaka, recimo, Zagreb-Split ugledate crnu ovcu kako pase i kažete: "Gle crnu ovcu!", prijatelj vas može ukoriti i kazati "Misliš, u Hrvatskoj postoji bar jedna ovca koja je bar s jedne strane crna?!". I zbog Dirichletova bi načela bio bliži istini.

Veliko poopćenje tog načela preraslo je u tzv. Ramseyevu teoriju, prema britanskom matematičaru F. Ramseyu koji se prvi time bavio oko 1930. godine.

Glavna ideja Ramseyeve teorije jest da je potpuni nered zapravo nemoguć, a svaki matematički "objekt" postoji negdje duboko ukopan ako ga potražite u dovoljno velikom univrezumu... Ramseyeva teorija uvijek traži najmanji univerzum u kojem pouzdano znamo da postoji izvjesni objekt. Jedan od glavnih promotora Ramseyeve teorije u 1950-ima bio je spomenuti Paul Erdös.

Vrlo je jednostavno opisati tipično pitanje Ramseyeve teorije. Koliki najmanji broj ljudi treba biti na "tulumu" tako da među njima sigurno postoji trojka međusobnih znanaca ili četvorka potpunih neznanaca? Pripadni najmanji traženi broj označimo s $R(3,4)$. Zna se da je $R(3,4)=9$.

(Pokušajte to sami dokazati. *Uputa.* Prvo dokažite da je $R(3,3)=6$.) Ramseyeva je teorija i dan danas "zona sumraka", tj. vrlo se malo o njoj zna. Na primjer ni danas se ne zna koliko je $R(5,5)$, koliko $R(5,6)$, a kamoli $R(10,7)$.

No, i ono malo što se u Ramseyevoj teoriji zna, Szemerédi je vrlo uspješno koristio u dokazivanju svojih teorema. Njegova su istraživanja već našla primjenu u umjetnoj inteligenciji i robotici. Za nadati se je da će naći primjene i u istraživanjima prirodne inteligencije (mozga), genetici i drugdje.

Čestitamo profesoru Szemerédiju na Abelovoj nagradi!